Europäisches Patentamt
European Patent Office
Office européen des brevets

Bescheinigung Certificate Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

02076389.2

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 02076389.2
Demande no:

Anmeldetag:
Date of filing: 09.04.02
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Semiconductor device, carrier, card reader, methods of initalizing and checking the authenticity

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

G01R/

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

Semiconductor device, carrier, card reader, methods of initializing and checking the authenticity

The invention relates to a semiconductor device provided with a circuit, a security layer that covers the circuit and a security element comprising a local area of the security layer and a sensor.

The invention also relates to a carrier provided with a semiconductor device and a card reader.

The invention further relates to a method of initializing and a method of checking the authenticity of the semiconductor device.

Such a semiconductor device and such a carrier are known from EP-A 300864. The security element of the known device is a capacitor with as sensor two capacitor electrodes that are coupled capacitively together by the security layer. The device comprises a plurality of security elements by preference. On checking the authenticity of the device, a measured voltage is compared to a calculated reference voltage. If there is a difference, the authenticity is not recognized. The carrier on which the device is present, is a smartcard.

It is a disadvantage of the known device, that the security elements may be circumvented. The security elements may be replaced by other structures with the same capacity which let the underlying circuit free. Further on, the removal of the security layer and the electrodes cannot be detected, if the electrodes and the security layer are reapplied afterwards. Such removal is done in order to look at, to probe electrically and/or to modify the circuit.

It is therefore a first object of the invention to provide a semiconductor device of the kind mentioned in the opening paragraph, of which removal of the security layer can be detected afterwards.

It is a second object of the invention to provide a carrier with an improved detection of hacking.

The first object is realized in that:

- the security layer comprises embedded magnetic particles, and

- the sensor is a magnetic sensor, therewith enabling measurement of a magnetic property of the security layer.

The second object is realized in that the carrier comprises the semiconductor device of the invention.

The use of magnetic particles has the advantage that they are in principal inert and that its properties are stable. Further on, it is not or hardly possible to provide after removal a security layer with the same magnetic properties as the original security layer. A removal of the security layer can be detected in that an actual value is compared to an initial value at an initialization that has been stored in a memory as reference value. The memory can be present in the semiconductor device. This has the advantage that one and the same value is available at two places in the semiconductor device, and that communication with an external, central database device is not necessary to check the authenticity. Alternatively, the memory can be present external to the semiconductor device. This has the advantage that it is not possible to modify the memory and the security layer, such that both the reference value and the actual value are different from the original values, but nevertheless equal. Preferably a plurality of security elements is present.

In a preferred embodiment, the magnetic sensor is a magnetoresistive sensor, therewith enabling the conversion of the magnetic properties into an impedance value. With the magnetoresistive sensor the magnetization that results from the distribution of the particles, are transformed into impedance values. Thus, the impedance can be measured on line. This has the advantage that any actual value of the impedance can be further processed, digitalized and stored in an easy and principally known manner. In the context of this application, the term 'impedance' relates to the impedance as measured in the magnetoresistive sensor. This impedance is in fact an impedance induced by momentaneous changes in the magnetisation in the security element. These changes can be provided by changing the magnitude of an external magnetic field, and especially by switching such external magnetic field on and/or off. The impedance of the magnetoresistive sensor is generally obtained as the difference between the sensor voltages in the reference state and in a magnetic field, which difference is divided by the sensor current used in the magnetoresistive sensor. The voltages are preferably the voltages of a Wheatstone bridge present in the sensor.

In a further preferred embodiment, the embedded magnetic particles are inhomogeneously distributed over the circuit. Due to the inhomogeneously distributed particles the security element has an impedance that is specific and unpredictable. The

inhomogeneous distribution of magnetic particles in the security layer over the circuit can be realized in various ways. If the layer is prepared from a particle suspension containing a solgel precursor, an inhomogeneity in the distribution of particles will naturally be present. This inhomogeneity can be further enhanced by variation in the suspension parameters, for instance by deliberately creating an unstable suspension. Another possibility is by deposition according to a desired pattern. It is advantageous that the suspension comprises a sol-gel precursor, such as a precursor for silica, titania, zirconia, or aluminophosphates. The inhomogeneity can be of chemical nature – e.g. chemically different magnetic particles or different compositions of magnetic particles – and of physical nature – e.g. different particle sizes, or otherwise.

In a further embodiment the inhomogeneous distribution is provided by the addition of non-magnetic particles. This has the result that not only the lateral position of the magnetic particles, but also or even mainly the vertical position of the magnetic particles varies over the circuit. As will be understood, the terms 'vertical' and 'lateral' are used in this context with respect to a plane of reference parallel to the security layer.

The magnetic particles can be any kind of magnetic particles, such as ferro-, and ferrimagnetic particles. Ferrite particles, such as $BaFe_{12}O_{19}$, could be used. If the nature of the precursor suspension is incompatible with the magnetic particles, the magnetic particles can be protected by encapsulation, for example in SiO_2 or in a polymer.

As is known to a person skilled in the art, magnetic particles can be subdivided on the basis of their hardness. A parameter for this hardness is the strength of the coercive field H_c. A second parameter characterizing the hardness of a magnetic material is the ratio R between the remanent magnetization M_r to the saturation magnetization M_{sat}. The remanent magnetisation is defined as the magnetization at zero external field, obtained after a magnetic saturation step. Softmagnetic materials that are suitable for transformers and inductors have a H_c that is small in an absolute sense and have $R<<1$. Magnetic materials with a larger H_c and a large R are used for magnetic recording or even as permanent magnets – together also referred to as hardmagnetic materials. Both soft- and hardmagnetic materials can be used in the device of the invention, however in different embodiments.

In a first embodiment, magnetic particles of a softmagnetic material are used, which particles have a diameter on a submicronscale, and preferably of less than 100 nanometer. Such particles are known as superparamagnetic particles and are ferro- and ferrimagnetic particles which are so small that, in the absence of an external field, their magnetisation fluctuates on a time scale that is much shorter than the time period during

which a magnetisation measurement is carried out. Preferably, a plurality of these particles is provided in an inert, micrometer-sized matrix, and as such present in the security coating. Such a matrix with superparamagnetic particles is commercially available and known as microbead. The softmagnetic material is for instance magnetite or a cubic ternary ferrite. With such materials a short measurement time of less than 1 second, preferably in the order of 0.001 – 0.1 seconds, can be realized. This is due to the small response time to the application of a magnetic field of superparamagnetic nanoparticles made of these materials. The response time is given by an Arrhenius expression, according to which the response time is an exponential function of the product of the magnetic anisotropy energy density and the particle volume.

The advantage of the superparamagnetic particles is that their magnetisation M fluctuates on a time scale that is much shorter than the time period in between of two measurements. As a consequence, the resultant magnetisation field $H_{//,Sx}$ parallel to the security layer and at a specific magnetoresistive sensor S_x can be assumed to be zero at the beginning of a measurement. Upon application of an external magnetic field, a magnetisation is induced in the direction parallel to this external magnetic field. This magnetisation induces a magnetic dipole field around the particles, which has a significant component perpendicular to the externally applied magnetic field and substantially parallel to the security layer. The resultant magnetisation field $H_{//,Sx}$ will be different and will induce changes in the resistivity of the magnetoresistive sensors. The magnitude of the resultant magnetisation field $H_{//,Sx}$ will be dependent on the amount of particles, the distance and location with respect to the magnetoresistive sensor.

In a second embodiment, particles of a hard-magnetic material – hard-magnetic particles - are used. The hard-magnetic particles can be of any kind or size, and preferably have an average diameter ranging from 0.1 to 3 microns. This average diameter is by far preference smaller than the thickness of the security layer, which however can be as thick as 10 microns or more.

Two sub-classes of hard-magnetic particles are distiguished. If the coercive field of the particles is much larger than the maximum field that can be allowed to be applied to the chip during its lifetime, the magnetization direction of each of the particles will be permanently fixed after magnetizing them once during the fabrication process. The measurement of the value of the security elements does then comprise the step of measuring the resistance of the sensor, without the application of an external magnetic field. This value is compared directly to the reference value obtained after the initialization step.

Within the second sub-class, an external magnetic field must be applied in order to induce the magnetisation. Within this second sub-class, the coercive field of the particles is smaller than or approximately equal to the maximum field that can be allowed to be applied during the lifetime of the chip. The application of a field larger than the coercive field changes the magnetic state of the particles. The particles must therefore prior to each measurement be brought into a reference state, in order to remove influences of any uncontrolled previously applied external magnetic field. A suitable example of a preliminary treatment is degaussing. In this treatment, generally applied in cathode ray tubes, an alternating magnetic field is applied. The strength of this field is initially equal to or larger than a saturation field of the hardmagnetic particles, but is reduced at every alternation to end at a standard value, in general a zero field.

The measurement of the value of the security elements with hardmagnetic particles within this second sub-class can be the same as for the particles of a softmagnetic material. This will comprise the steps of measuring a resistance of the sensor at a reference state in zero applied field, applying an external field in a direction substantially perpendicular to the plane of the security layer, said external field having a strength of at least the saturation magnetic field, and measuring the resistance again. The second measurement is preferably started after the resultant magnetisation field $H_{//,Sx}$ has reached its saturation value and stopped before the external field is switched off.

Alternatively, with the advantage that the level of security is enhanced, and with the advantage that the application of the external field has no or a weaker direct influence on the resistance of the sensor, the external field can be zero or of a strength below the saturation magnetic field of the hardmagnetic particles. In a phase prior to the measurement the field can further be applied in a degaussing manner to end up around said bias value below the saturation magnetic field. Subsequently, a measurement is carried out. A special case is that in which the measurement is carried out at zero field.

It is possible to create a well defined remanent state of the magnetic particles that is different from that in the reference state by making use of a variation with time of the external field prior to the measurement that is different than that used for obtaining the reference state. The resultant resistivity that is measured is thus not only dependent on the size and specific distribution of the magnetic particles in the security layer, but also on their detailed hysteretic magnetic response to a time dependent magnetic field. This enhances the level of security for two reasons. Firstly, a prediction of the remanent magnetization of a particle after a degaussing procedure on the basis of a measurement of only the volume and

of the full hysteresis loops is in practice impossible, because the so-called inner hysteresis loops depend on detailed internal magnetic states of the particle that are not probed when measuring a full magnetization loop, and because such inner loops are already strongly modified by weak and in practice non-detectible random variations of the particle properties. Secondly, the sensor responses obtained after many different degaussing procedures can be compared to those obtained in a corresponding way in initialization procedure. Such responses are very specific and are to be considered as a 'magnetic signature'. The degaussing procedures can be varied in length and character as will be clear to the skilled person in that field. Also, use can be made of the full time dependence of the response.

In a further embodiment, superparamagnetic particles, or a mixture of such particles, are chosen such, that its or their relaxation time is comparable to the measurement time. As a consequence the time dependence of the resistivity can be used in addition to the absolute value of the resistivity. This time dependence of the resistivity can be measured by the magnetoresistive sensors after the application of a – sudden - fixed magnetic field.

In an advantageous embodiment the first security element comprises a Wheatstone-bridge having a first pair of magnetoresistive sensors and a second pair of sensors, the sensors of which first and second pair are provided with substantially the same resistance versus magnetic field characteristic. Such characteristic is implemented through the physical and the magnetic structure, e.g. the sensors have the same size and contain the same material, and the pinned layer is in all the sensors of the bridge pinned in the same direction. Through the use of a Wheatstone bridge the sensitivity of the security element for variations in the impedance is increased, since not the impedance itself, but a difference in impedance between the first and the second magnetoresistive sensors of the first pair – and optionally the second pair – is measured. Besides, with a Wheatstone bridge the measurement is independent of temperature changes, and compensates for a constant background field. This Wheatstone bridge is known per se by the person skilled in the art of magnetoresistive sensors. The term Wheatstone bridge is understood to include, in the context of this application, a so-called half Wheatstone bridge comprising a first pair of magnetoresistive sensors and a second pair of identical non-magnetic elements; a full Wheatstone bridge including a first and a second pair of magnetoresistive sensors; and any variant on a Wheatstone bridge. The magnetoresistive sensors can be of various type, such as GMR, TMR and AMR and are known per se. Next to a standard magnetoresistive sensor as is described with reference to the drawings more complex sensors can be used. Examples thereof are spin valves with dusting layers, specular spin valves, spin valves with artificial antiferromagnets

as pinned layers. If there is a passivation layer under the security layer, the magnetoresistive sensors may be present on either side of this passivation layer.

In a further embodiment the security element has a construction that the magnetoresistive sensors having an axis of sensitivity substantially parallel to the security layer are shaped as stripes that have a length in a direction substantially perpendicular to the axis of sensitivity. The magnetoresistive sensors of this embodiment are robust in the sense that a deviation of the magnetic field from the direction perpendicular to the security layer is not harmful. Generally such a deviation is harmful if it saturates the sensor.

Preferably, the passivation structure comprises a plurality of security elements. These elements can all be security elements comprising at least one magnetoresistive sensor. However, it can be as well, that various types of security elements are present. Other types of security elements include capacitors, resistors, inductors and combinations thereof, wherein the passivation structure comprises a layer with a varying dielectric constant laterally over the circuit.

As will be explained in more detail below, the impedance measured in the security element must be converted into a signal that can be stored in a memory, either inside the semiconductor device or in any reader or database connected to the reader. For this aim, conversion means are present to convert an output voltage from the first security element into an actual value of the first impedance. The conversion means may be of well-known nature, such as an A/D-converter or any circuit based on a comparison with a pre-determined clock-frequency.

The carrier of the invention may be a smartcard, a record carrier such as an optical disc, a security paper such as a banknote.

It is a third object of the invention to provide a card reader with which the authenticity of the semiconductor device of the invention can be checked.

The third object is realized in a card reader suitable for a card with a semiconductor device of the invention, in which card reader magnetisation means are present in order to generate an external magnetic field that will induce a magnetisation in the magnetic particles substantially perpendicular to the security layer. The external magnetic field to be generated has preferably a strength in the order 10-100 kA/m. Examples of magnetisation means include a coil and a permanent magnet. If a coil is used, it may be provided with a core, for instance of ferrite material. Further on, a number of coils or magnets that are placed in parallel to each other, and are electrically connected in series may

be used. Such a construction appears advantageous in that a field in substantially one direction is generated. A preferred number is two if a field in one direction is desired. If a field in three directions is desired, the preferred number is six. The actual card reading part of the card reader is preferably present in between of the coils or magnets of the magnetisation means.

Preferably a reference sensor is present in de card reader in order to measure the external magnetic field. With said measurement the magnetic field can be calibrated. Further on, the card reader may contain heating means, such as an infrared lamp or another local heat source, or the provision of a flow of fluid or gas at a specified temperature. A thermometer may be present as well.

In a further embodiment, the coil of the card reader is part of a degaussing circuit. Such a degaussing circuit is per se known from the art of cathode ray tubes. It may be used to provide an adequate magnetisation of permanent magnetic particles, such that any prior existing magnetisation becomes irrelevant. A preferred example of a degaussing circuit comprises a dual PTC thermistor, and a shunt capacitor parallel to the coil to prevent disturbances.

It is a fourth object to provide a method of initializing the semiconductor device of the invention.

It is a fifth object to provide a method of checking the authenticity of the semiconductor device of the invention.

The fourth object is realized in a method of initializing the semiconductor device of the invention, in that

determining an initially actual value of the impedance of the security element, and

storing the initially actual value as the reference value in a memory.

The fifth object is realized in a method of checking the authenticity of the semiconductor device of the invention, the device being initialized, comprising the steps of:

- determining an actual value of the impedance of the security element, and
- reading the reference value from the memory,
- comparing the actual value and the reference value, and
- recognizing the authenticity of the semiconductor device only, if the difference between the actual value and the reference value is smaller than a predefined threshold value.

The method of initializing the semiconductor device is necessary, in that before the initialization no actual value of the impedance of the security element is known.

The method of checking the authenticity has the advantage that both the actual value and the reference value are available and can be compared. The actual value is available and physically fixed in the semiconductor device. The reference value can be available in the semiconductor device, but is alternatively available in a central database device to which the card reader has access, or which is incorporated in the card reader. The reference value could also be present both in the semiconductor device and in the central database device. It will be understood that the method can be repeated in case that a plurality of security elements is present.

The predefined threshold value is generally very small, e.g. preferably below 5% of the reference value, and to be defined in order to correct uncertainties of measurements or influences of temperature and other external conditions. It is being mentioned that under normal conditions there will be a plurality of security elements, each with their own impedances. It can thus be expected that all impedances, or at least a part of them, must be compared to the corresponding reference values, before the authenticity of the semiconductor device can be recognized completely.

If the reference value is stored in a memory of the central database device, the method of checking the authenticity can be interpreted as a method of identifying the semiconductor device as well; e.g. instead of checking whether the actual value is equal to the reference value belonging to an already known identity of the semiconductor device, the actual value can be used to find a corresponding reference value in the database, and therewith the identity of the semiconductor device. The use of the reference values in connection with a central database device is generally referred to as a unique chip identifier code.

In a preferred embodiment, the step of determining the actual value comprises the steps of:

- measuring an off-state value at a standard external magnetic field;
- generating an external magnetic field to induce a magnetisation in the magnetic particles substantially perpendicular to the security layer;
- measuring an on-state value before the external magnetic field is switched off,
- determining an actual value of the impedance as the difference between the on-state value and the off-state value,

As explained above, only the magnetic particles of which the magnetization can be permanently fixed, can be measured directly. For other magnetic particles it is necessary to apply an external magnetic field before measuring. This external field is

preferably generated in the card reader. In order to have a calibrated actual value, it is measured as the difference between an off-state value at standard, preferably zero external field, and an on-state value at the external magnetic field.

In the case that the magnetic particles or at least part thereof contain a hard-magnetic material, a preliminary treatment is necessary to remove existing magnetisation in the magnetic particles in the direction substantially perpendicular to the security layer. Such a preliminary treatment can be a degaussing treatment, such as described above in more detail.

In the case that the magnetic particles or at least part thereof contain a soft-magnetic material, a relaxation measurement can be done comprising the steps of:

- generating an external magnetic field to induce a magnetisation in the magnetic particles substantially perpendicular to the security layer;
- measuring a first and a second value before the particles of the softmagnetic particles are relaxated to their saturation magnetisation, and
- determining the actual value of the impedance of the security element as the difference between the first and second value.

This relaxation measurement offers a specific response. The number of values to be measured depends on the relaxation time of the soft-magnetic material, which is known per se. The actual value is determined as the difference between the second and first value, in order to correct for drift effects. If a large number of values is measured, the difference can be calculated between the measured value and the first value, or between consecutive values. The measurement can be optimized in that after measuring the first and second value an external magnetic field is generated in the opposite direction and further values are measured.

These and other aspects of the semiconductor device and the methods of initializing it and checking its authenticity according to the invention will be further explained with reference to the drawings, in which:

Fig. 1 shows a diagrammatical cross-section of the semiconductor device;

Fig. 2 shows a diagrammatical cross-section of a security element in the semiconductor device;

Fig. 3A shows a diagrammatical top-view of the security element;

Fig. 3B shows a electrical scheme corresponding to the security element shown in Fig. 3A

Fig. 4A-C show graphs of the applied field, the magnetisation and the measured voltage difference as a function of time for the embodiment with magnetic particles of superparamagnetic material;

Fig. 5A-C show graphs of the applied field, the magnetisation and the measured voltage difference as a function of time for the embodiment with magnetic particles of hard-magnetic material, wherein measurement takes place at the saturation field;

Fig. 6A-C show graphs of the applied field, the magnetisation and the measured voltage difference as a function of time for the embodiment with magnetic particles of hard-magnetic material, wherein measurement takes place at a field of less than the saturation field; and

Fig. 7 shows a schematic diagram of the semiconductor device.

The figures are schematically drawn and not on scale, and the equal reference numbers in different figures refer to corresponding elements. It will be clear to the person skilled in the art, that alternative but equivalent embodiments of the invention are possible within deviation of the true inventive concept, and that the scope of the invention will be limited by the claims only.

In Figure 1 the semiconductor device 11 has a substrate 31 of silicon, having a – first - side 32. On this side 32, the device 11 is provided with a first active element 33 and a second active element 43. These active elements 33, 43 are in this example bipolar transistors with emitter regions 34, 44, base regions 35, 45 and collector regions 36,46. Said regions 34-36, 44-46 are provided in a first layer 37, which is covered with a patterned insulating layer 38 of silicon oxide. The insulating layer 38 is patterned such that it has contact windows at the emitter regions 34, 44 and the base regions 35, 45. As known to those skilled in the art, field effect transistors can be present instead of or besides the bipolar transistor. As further known to those skilled in the art, other elements, such as capacitors, resistors and diodes can be integrated in the semiconductor device 11. The active elements are interconnected so as to form a circuit.

At these contact windows in the insulating layer 38, the said regions are connected to interconnects 39, 40, 41, 42. The interconnects in this embodiment extend on a first level and a second level. As is generally known, the interconnect structure can contain more levels. Between the interconnects and the active elements a not-shown barrier layer is generally present. The interconnects 39, 40,41,42 are manufactured, for example in Al or in Cu, in a known manner and are covered and mutually insulated through dielectric layers 47,

that preferably have a low dielectric constant. Additionally present barrier layers are not shown. A third level interconnect 28 is present to connect the security element 12, comprising a first and a second magneto-resistive sensor 121, 122 and a local area of a passivation structure 50.

This passivation structure 50 contains in this embodiment a passivating layer 52 of Si_xN_y in a thickness of 0.60 μm. Under the passivating layer 52 a further layer of phosphosilicateglass can be present. The passivation structure further contains a security layer 53 of aluminophosphate in a thickness of 2-10 μm, in which magnetic particles are embedded. Also TiO_2 and TiN particles are present in order to stabilize the security layer 53, and to decrease the transparency of the layer. A not-shown planarizing layer may be present below the passivating layer 52. This security layer 53 was applied by spincoating a composition of 15 % by weight monoaluminumphosphate, 20-50% by weight of particles in water, and subsequent drying at about 100-150 °C. Alternatively, it can be applied by spraycoating a composition of 5-10% by weight monoaluminumphosphate. After drying, the layer is annealed at 400-500 °C to allow condensation, due to which a transition from the fluid to the solid phase takes place. On the security layer 52 an epoxy material is present as package 54. The security layer 53 may be patterned, so as to facilitate sawing of the wafer into separate dies, and to define contact pads for connection to a PCB for example.

The sensors 121, 122 are at a mutual distance of about 1 micrometer. Their functioning will be explained in more detail with reference to the figures 2 and 3. The sensors 121,122 may be present at larger mutual distances. If however the distance is smaller than 2 microns, the measurement in improved. This is due to the fact that magnetic particles that are present in between of the sensors will induce magnetisations in opposite directions in the sensors, and thus to different changes in the impedance.

Fig. 2 shows a diagrammatical cross-section of a detail of the security element 12; The magnetoresistive sensors 121, 122 comprise each a stack of four main layers: a pinning layer 61, a pinned layer 62, a spacer layer 63 and a free layer 64. The pinning layer 61 is an antiferromagnet, in this case a 10nm thick $Ir_{20}Mn_{80}$ layer. It may be insulated from the underlying structure through one or more buffer layers, such as 3 nm thick layers of Ta and/or $Ni_{80}Fe_{20}$. The pinned layer 62 – in this case 6 nm Co - has a magnetisation that is not variable due to the influence of the pinning layer 61. It is preferred that the magnetisations of the pinned layer 62 of the magnetoresistive sensors 121, 122 are in parallel directions. The output voltage of the bridge is then not sensitive to a uniform external magnetic field. The spacer layer 63 comprises in the preferred case of a GMR sensor a conductive material, such

as Cu with a thickness of 3 nm. In the case of a TMR sensor an insulating material such as Al_2O_3 with a thickness of 1 nm is applied. The free layer 64 comprises a soft-magnetic material like $Ni_{80}Fe_{20}$ in a thickness of about 6 nm.

Fig. 2 shows the situation that in the security layer 53 there are three superparamagnetic particles present near to the magnetoresistive sensors 121,122, of which the axis of sensitivity is parallel to the direction of the magnetization in the pinned magnetic layers 62 (the x-axis). The particles are of different size and are present at different distances and angles with respect to the sensors 121,122. After application of a magnetic field that is oriented perpendicular to the plane, with a time dependence that will be further explained with reference to Fig.4, a perpendicular magnetisation will be induced in the particles.This result in a dipolar field around the particle, as indicated in the figure schematically by magnetic field lines. The dipolar field from the magnetic particles A, B and C will exert a magnetic torque on the magnetization of the free layers 64 of the sensors 121, 122, which in the absence of the dipolar fields are oriented substantially parallel to the y-direction (i.e. the direction perpendicular to the plane of the paper). The torque depends on the distance along the x and z (perpendicular to the layer plane) directions between the particles A, B, C and the sensor, and is proportional to the strength of the magnetisation of the particles A,B,C. As a consequence, rotations of the magnetisations are induced in the free layers 64. The directions and sizes of these magnetisation rotations are determined by the directions and sizes of the effective (layer averaged) x-components of the magnetic fields induced by the magnetic particles A,B,C. The magnitude of these fields, at distinct positions in the sensor plane, is in the figure indicated through the lengths of the arrows. As a consequence, there is a net magnetisation rotation to the right (i.e. towards the positive x-direction) in the first sensor 121 and a net magnetisation rotation to the left in the second sensor 122. The net x-component of the magnetisation of the free layer 64 in the first sensor 121 is therewith larger than that of the free layer 64 in the second sensor 122. The resistance of the magnetoresistive sensors 121,122 depends on the angle between the magnetization directions of the the pinned and the free layer 62,64. As a consequence, the resistance of the sensor 121 is decreased compared to average, whereas the resistance of the sensor 122 is increased.

Fig. 3a shows a diagrammatic top-view of the security element 12. Fig. 3b shows an equivalent electrical scheme. The security element 12 is a Wheatstone bridge. The parts 123, 124 can be either equal non-magnetic resistors or magnetoresistive sensors, preferably of the same type as sensors 121, 122. Although preferred, it is not necessary that the parts 123,124 have the same physical dimensions as the sensors 121,122. The security

element 12 includes next to the parts 121-124 and the non-shown security layer electrodes 131-134. The first electrode 131 is current input, the second and the third electrode 132,133 are mutually connected via a voltage measurement. Conversion means are present to convert an output current or voltage from the security element into an actual value of the impedance. The conversion means will be further explained with reference to Fig. 7. The fourth electrode 134 is current output. It is observed that the shape of the Wheatstone bridge as shown in Fig.3a is not essential for the embodiment. This is due to the randomness of the distribution of the magnetic particles.

Figures 4, 5 and 6 show graphs of the applied field, the magnetisation and the measured voltage difference for three embodiments of the invention. Figure 4 relates to the embodiment with superparamagnetic particles. Figures 5 and 6 relate to the embodiment with hardmagnetic particles of which a reference state is defined prior to the measurement. In Figure 5 measurement at the saturation field is shown, whereas in Figure 6 measurement at a degaussed field of less than the saturation field is shown.

When using superparamagnetic particles the magnetisation of the particles is zero before the application of an external field. Therefore one can do a off-state measurement of the output voltage of the Wheatstone bridge immediately. This measurement will begin at $t_{R,B}$ and end at $t_{R,E}$. Thereafter one applies the external magnetic field H_{app} at t_0. This will lead to an increase of the magnetisation of the particles M to its saturation value M_{sat}, on a time scale that is determined by the relaxation time or the relaxation time distribution of the particles. Thereafter, the magnetisation is stable as long as the field H_{app} is present, and a measurement of the voltage difference ΔV can be done. This on-state measurement will begin at t_B and end at t_E. Finally at t_1, the external magnetic field H_{app} will be switched off and the magnetisation M and the voltage difference ΔV will reduce to their reference values. The actual value is determined as the difference between the on-state measurement and the off-state measurement. Alternatively, the measurement of the voltage difference can be carried out as a function of the time. This is of most interest if the relaxation time is of the order of the time t_1.

When using hard-magnetic particles of which the coercive field is smaller than or of the same order of magnitude as the maximum uncontrolled external field that is allowed, a pretreatment is necessary to remove any remanent magnetisation. A preferred method therefore is a degaussing treatment. In such a degaussing treatment, as shown in Fig. 5A, an oscillatory external magnetic field is applied with alternating directions and decreasing maximum strengths. Thereafter the off-state measurement is done, the external

field H_{app} is applied at t_0 and the on-state measurement is done from $t_{B,1}$ to $t_{E,1}$. The actual value is again determined as the difference between the on-state and the off-state value. After switching off the field H_{app} at t_1, a remanent magnetisation will still in general be present. This remanent magnetisation, which is a materials' property, can be used for an additional measurement, from $t_{B,2}$ to $t_{E,2}$.

Alternatively, the measurement can be preceded by a degaussing treatment in a specified manner that is different from that used for obtaining the reference state, e.g. degaussing around a certain bias field, as is shown in Figure 6. The subsequent measurement can take place at a finite field, e.g. the bias field around which degaussing has taken place. It can also take place after switching off the external final field.

Fig. 7 shows a schematic diagram of an embodiment of the semiconductor device 11 together with an access device 2. The semiconductor device 11 comprises various means: measuring means 4, memory 7, control means 8 and a verification control 9. Further on, the semiconductor device comprises a plurality of security elements 12, as well as a switch 10. The memory 7 comprises a plurality of memory elements 7A, 7B, 7C... ., as well as a storage control 5 and read control 6. The control means 8 and the verification control 9 may be integrated into one function, this being a microprocessor, or a dedicated circuit. The control means 8 need not to be dedicated solely to the control of the measuring, storing and reading of the impedances of the security elements 12, but may control the functioning of the complete semiconductor device, including a further memory with financial or identity data. The access device 2 is generally a card reader, but may be another device, for instance an apparatus with which the initialization is done.

The exemplary circuit in the semiconductor device 11 functions as follows: a signal is sent from the access device 2 to the semiconductor device 11, requesting the initialisation or authenticity check. Via control means 8 values of the impedances of the security elements 12 are measured, and with a frequency depending on the impedance they are sent to conversion means 4, and then via a switch 10 to the memory 7. The conversion means generally include an oscillator, a counter and a reference oscillator to provide a clock frequency, or a standard A/D converter. The result is a digitalized signal, that is the actual value of the impedance of the measured security element. It may be present in any kind of SI-unit, but also in any device specific value, if it is not to be compared with any externally measured value. Depending on the switch 10, the actual value may be stored or provided to the verification control 9. The switch is preferably switchable only once, for example in that it comprises a fuse. It is not excluded, as will be apparent to the skilled person, that the

switch 10 and the storage control 5 are integrated into one functional unit. The verification control 9 will compare the actual value and the reference value. If the difference between both values is smaller than a predefined threshold value, for instance 3%, then a positive signal – stating okay - will be sent to the control means 8. This can be done immediately, or after comparing all the actual values with all reference values, or after comparing a selected number of the actual values with the corresponding reference values. The predefined threshold value will be dependent on the precision of the measuring means. It could be 10 or 20% as well, especially if the number of security elements is large, for instance 10 or more. It could be less than 1% as well, which is partially dependent on the customer's wishes and the state of the art of integrated circuit design.

CLAIMS:

1. A semiconductor device provided with a circuit, a security layer that covers the circuit and and a security element comprising a local area of the security layer and a sensor,
characterized in that:

- the security layer comprises embedded magnetic particles, and
- the sensor is a magnetic sensor, therewith enabling measurement of a magnetic property of the security layer.

2. A semiconductor device as claimed in Claim 1, characterized in that the magnetic sensor is a magnetoresistive sensor, therewith enabling a conversion of the magnetic properties into an actual value of the impedance.

3. A semiconductor device as claimed in Claim 1, characterized in that the embedded magnetic particles are distributed inhomogeneously in the security layer (53) over the circuit.

4. A semiconductor device as claimed in Claim 1, characterized in that the magnetic particles are superparamagnetic particles embedded in microbeads.

5. A semiconductor device as claimed in Claim 1, characterized in that the magnetic particles contain a hard-magnetic material.

6. A semiconductor device as claimed in Claim 2, characterized in that the magnetoresistive sensors having an axis of sensitivity substantially parallel to the security layer are shaped as stripes that have a length in a direction substantially perpendicular to the axis of sensitivity.

7. A semiconductor device as claimed in Claim 1, further provided with a memory to store an initially actual value of the impedance of the security element as reference value.

8. A carrier provided with a semiconductor device according any of the Claims 1-7.

9. A card reader suitable for a carrier according to Claim 8, characterized in that magnetisation means are present in order to generate an external magnetic field that will induce a magnetisation in the magnetic particles substantially perpendicular to the security layer.

10. A card reader as claimed in Claim 9, characterized in that a reference sensor is present for measuring the external magnetic field, so that the external magnetic field can be calibrated.

11. A card reader as claimed in Claim 9, characterized in that the magnetisation means are part of a degaussing circuit.

12. A method of initializing the semiconductor device according to any of the Claims 1-7, comprising the steps of:

- determining an initially actual value of the impedance of the security element, and
- storing the initially actual value as the reference value in a memory in the semiconductor device or in a central database device located in or connected with the card reader according to Claim 9.

13. A method of checking the authenticity of a semiconductor device according to any of the Claims 1-7, the device being initialized according to the method of Claim 12, comprising the steps of

- determining an actual value of the impedance of the security element, and
- reading the reference value from the memory,
- comparing the actual value and the reference value, and
- recognizing the authenticity of the semiconductor device only, if the difference between the actual value and the reference value is smaller than a predefined threshold value.

14. A method of initializing or checking as claimed in Claim 12 or 13, characterized in that the step of determining an actual value comprises the steps of:

- measuring an off-state value at a standard external magnetic field;
- generating an external magnetic field to induce a magnetisation in the magnetic particles substantially perpendicular to the security layer;
- measuring an on-state value before the external magnetic field is switched off,
- determining the actual value of the impedance of the security element as the difference between the on-state value and the off-state value.

15. A method of initializing or checking as claimed in Claim 14, characterized in that:

- at least part of the magnetic particles embedded in the security layer of the semiconductor device contain a hardmagnetic material; and
- before measuring the off-state value a preliminary treatment is done in order to remove existing magnetisation in the magnetic particles in the direction substantially perpendicular to the security layer.

16. A method of checking the authenticity as claimed in Claim 15, characterized in that the external magnetic field is generated at a strength below the saturation magnetisation field of at least part of the magnetic particles.

17. A method of checking the authenticity as claimed in Claim 15, characterized in that the external magnetic field is alternating, while the magnitude of the field decreases to end up at a average bias field below the saturation magnetisation field of at least part of the magnetic particles.

18. A method as claimed in Claims 12 or 13, characterized in that at least part of the magnetic particles embedded in the security layer of the semiconductor device contain a soft-magnetic material and that the step of determining an actual value comprises the steps of:

- generating an external magnetic field to induce a magnetisation in the magnetic particles substantially perpendicular to the security layer;

- measuring a first and a second value before the particles of the soft-magnetic particles are relaxated to their saturation magnetisation,
- determining the actual value of the impedance of the security element as the difference between the first and second value.

ABSTRACT:

The semiconductor device has a security coating with embedded magnetic particles and magnetoresistive sensors. This allows measurement of the impedance of security elements defined by magnetoresistive sensors and security coating. If initial values of the impedance are stored, actual values can be compared therewith to see if the device has not been electrically probed or modified. Such comparison can be used to check the authenticity of the device.

Fig. 1

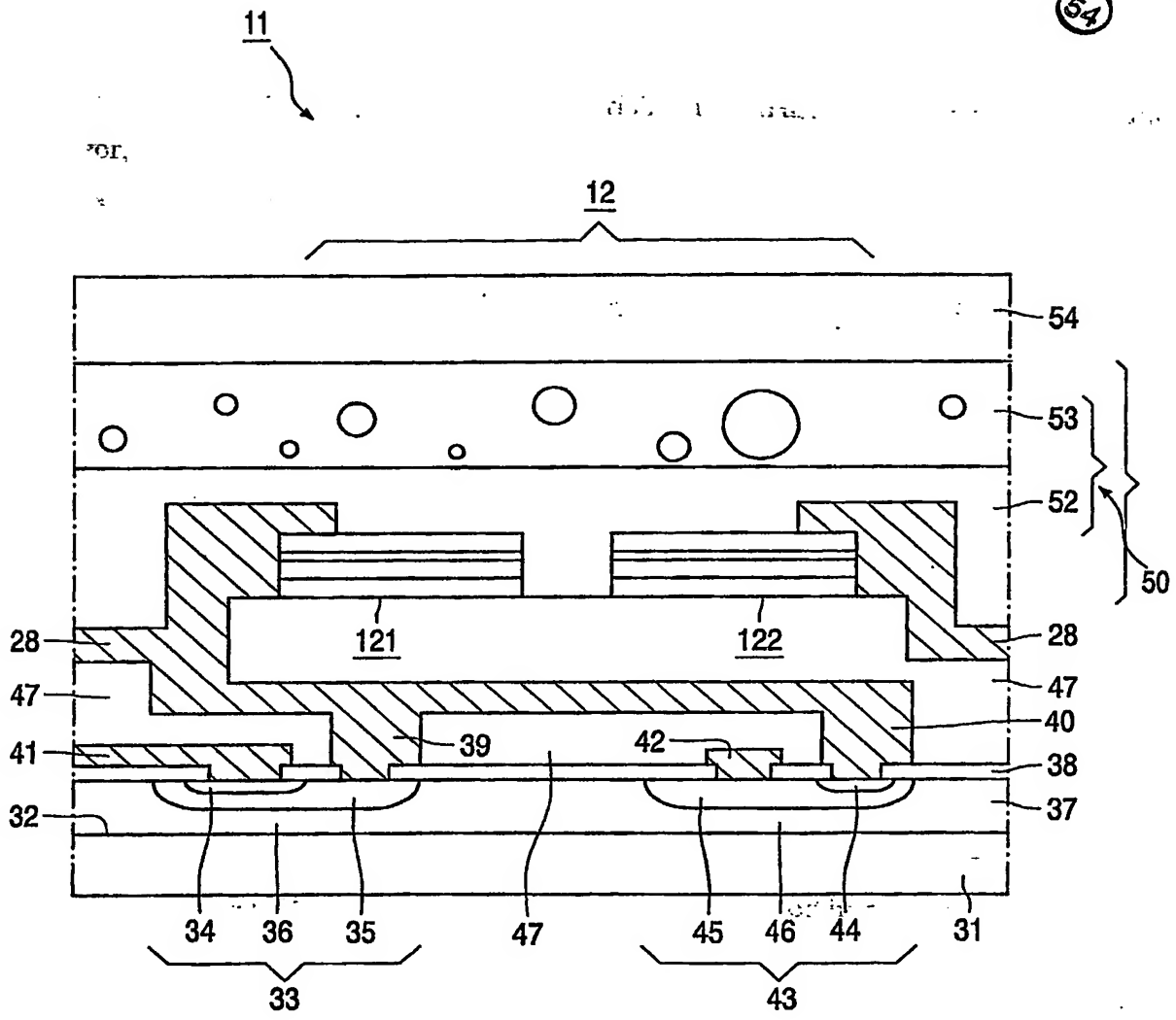

FIG. 1

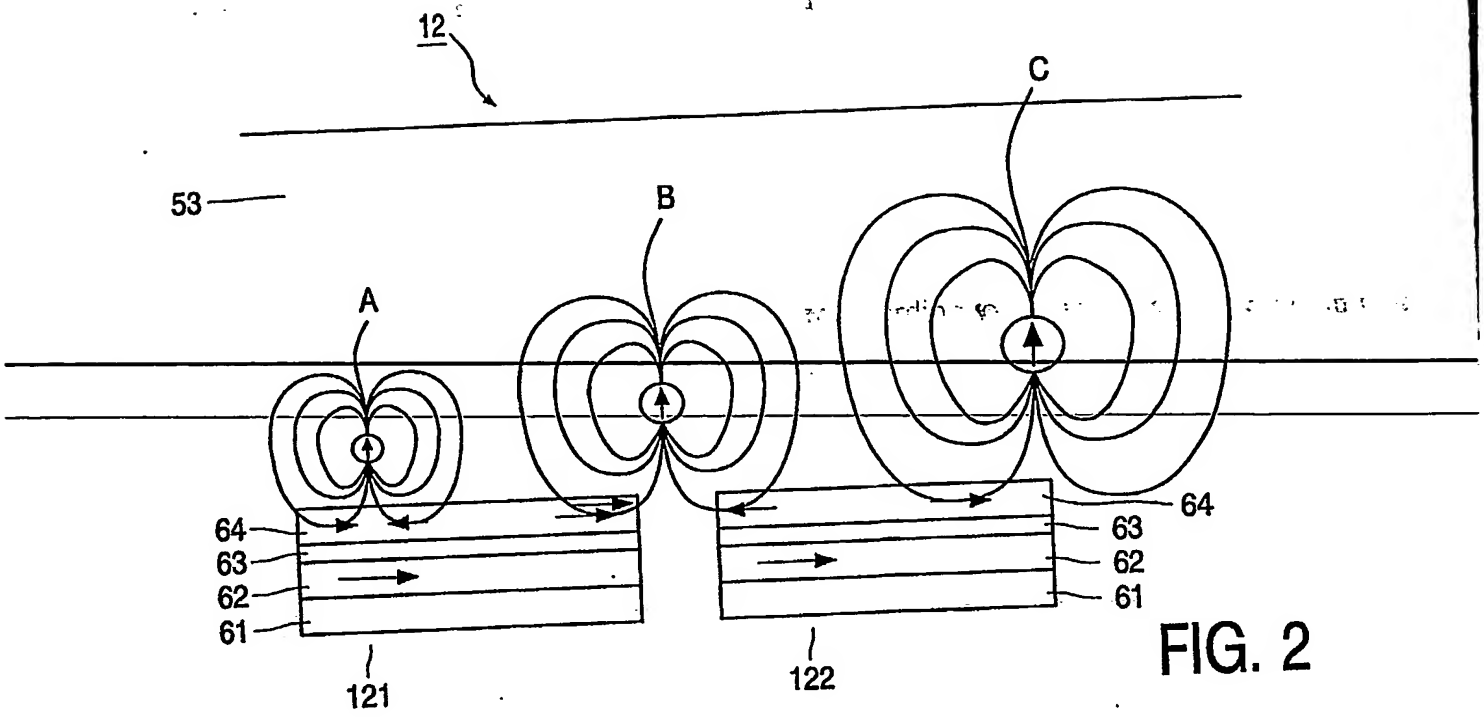

FIG. 2

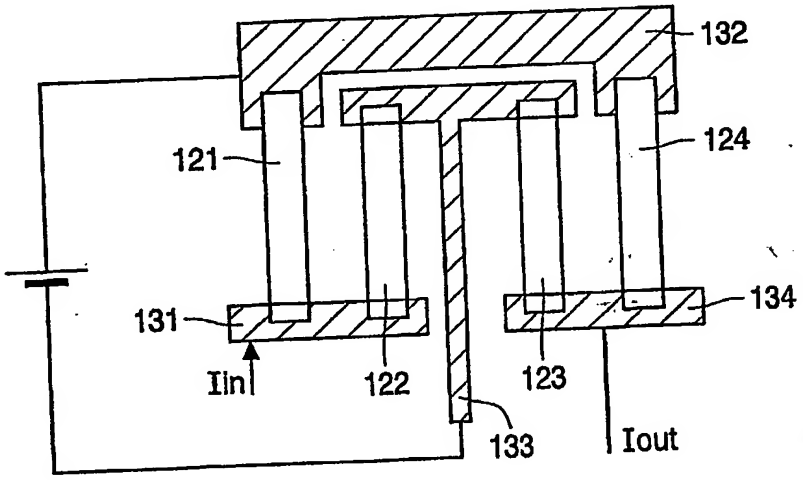

FIG. 3A

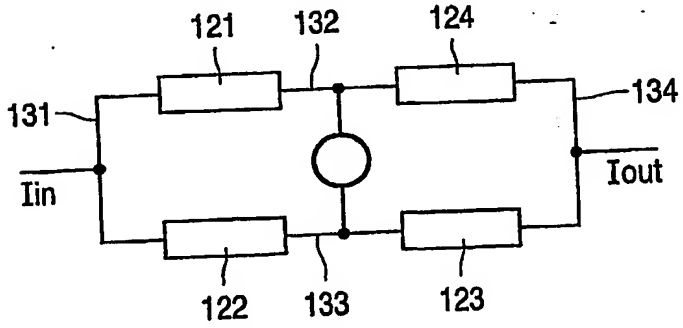

FIG. 3B

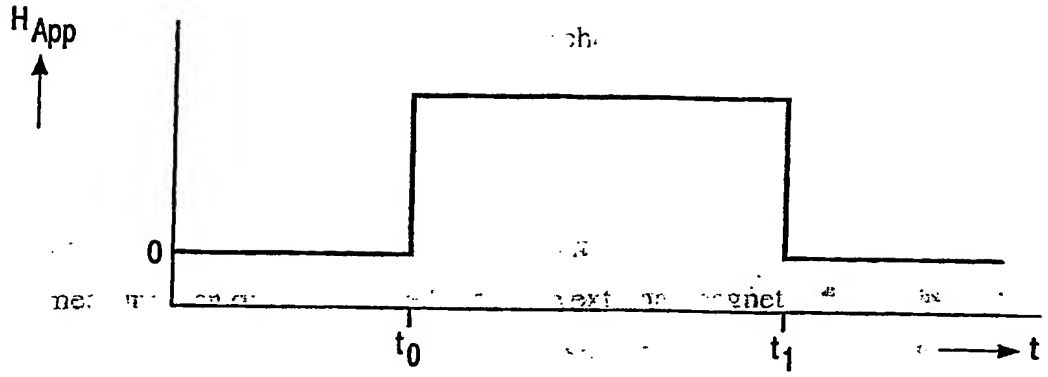

FIG. 4A

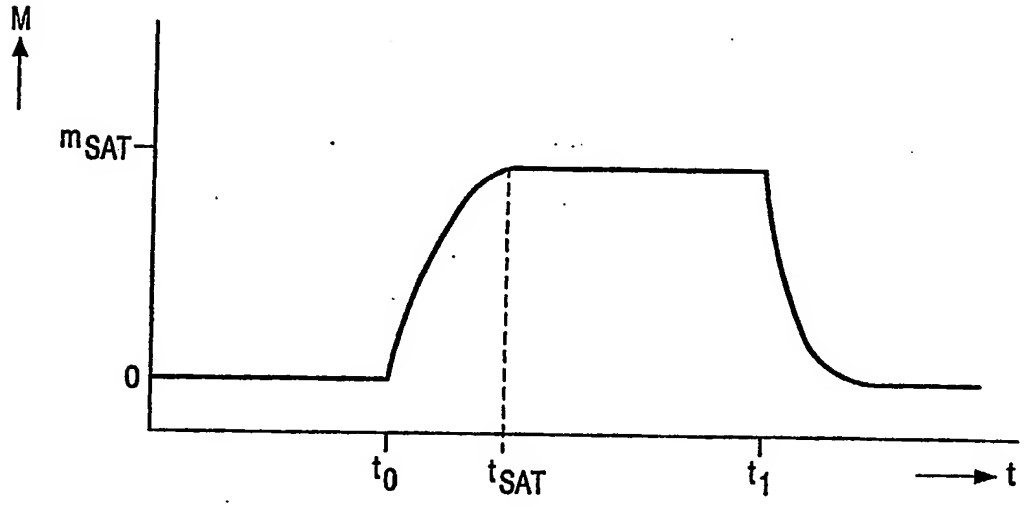

FIG. 4B

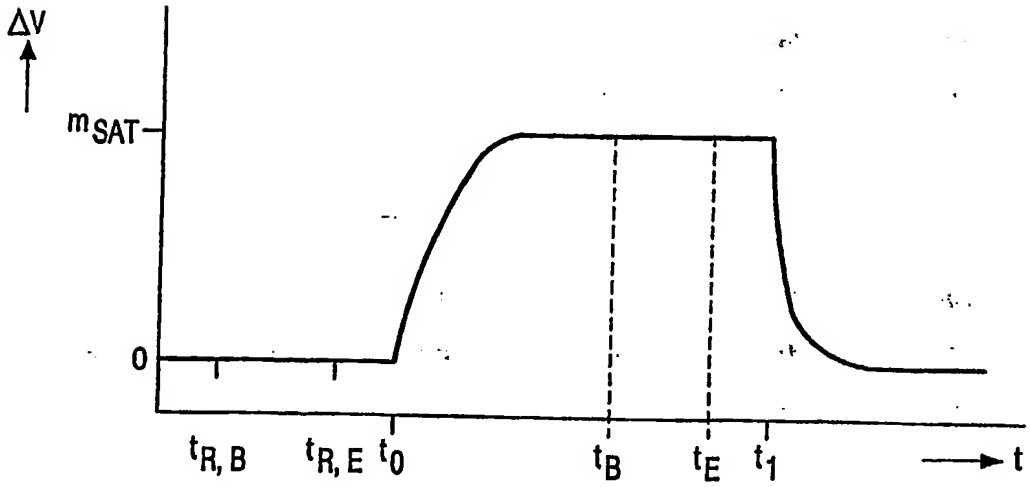

FIG. 4C

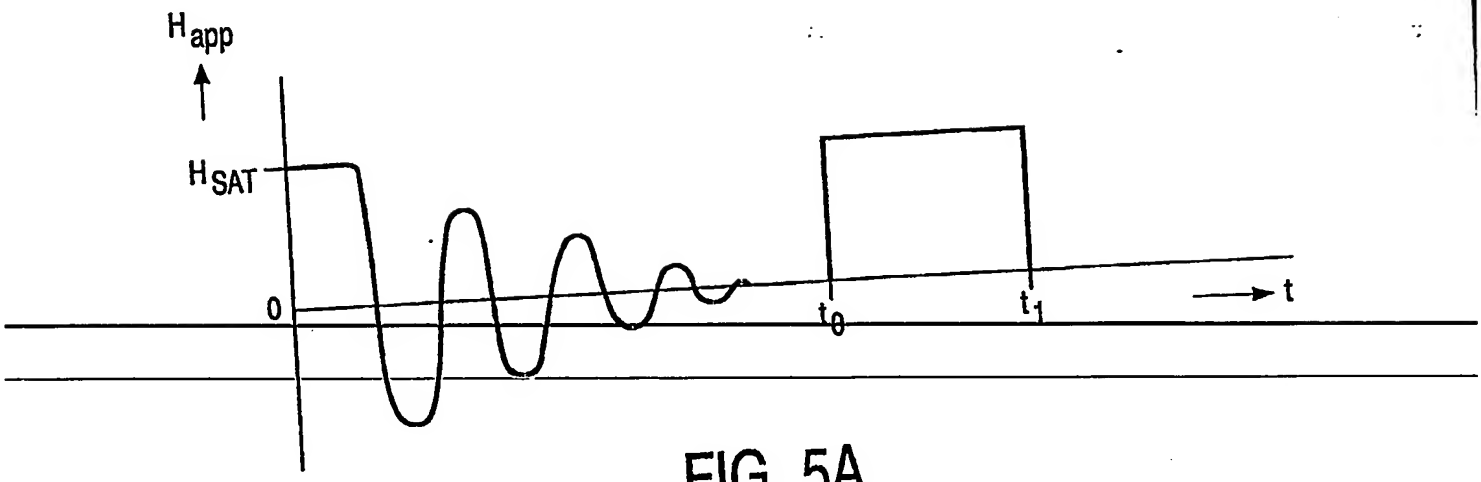

FIG. 5A

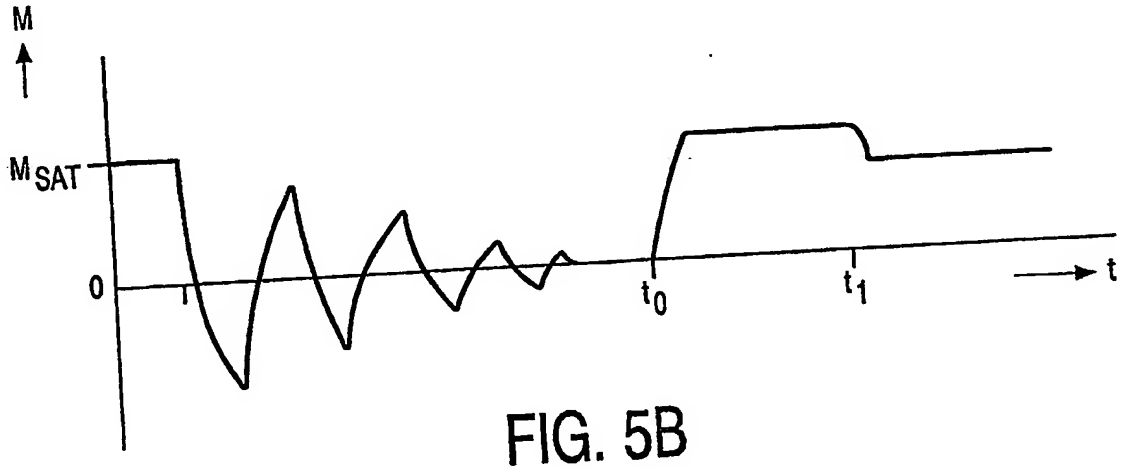

FIG. 5B

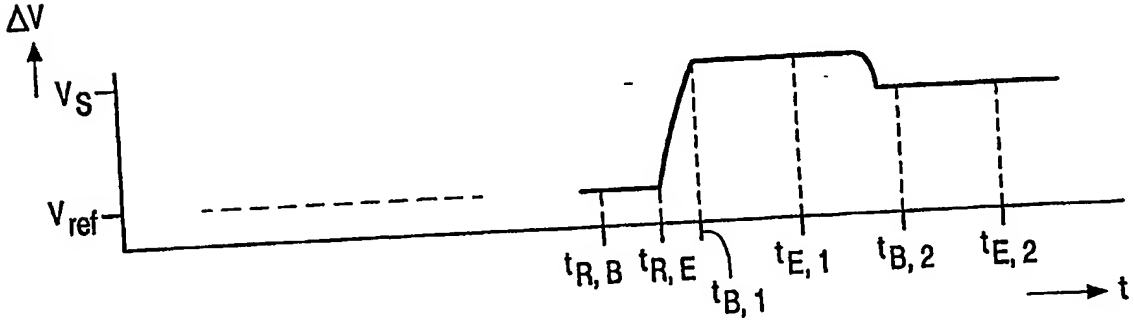

FIG. 5C

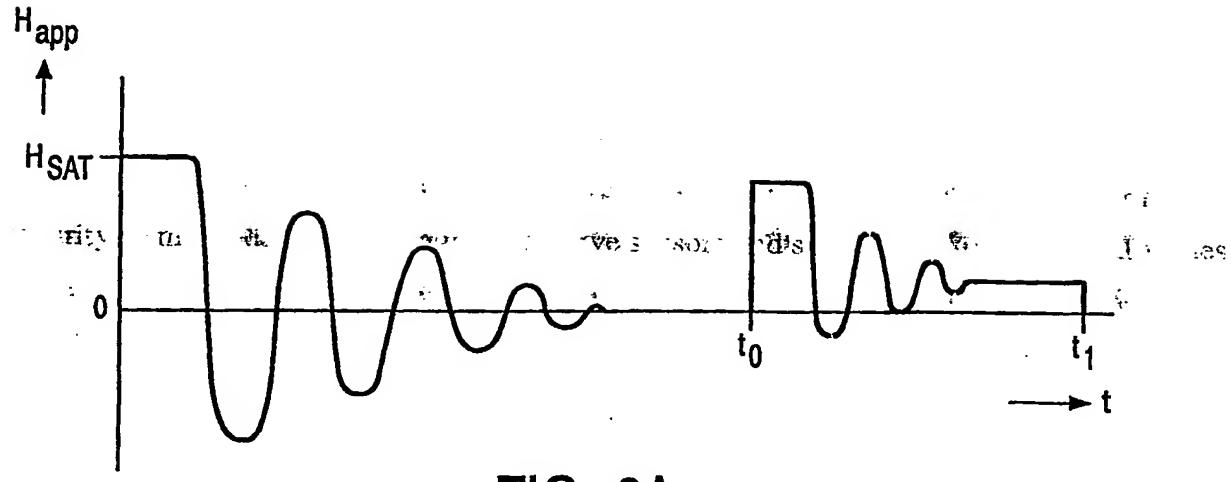

FIG. 6A

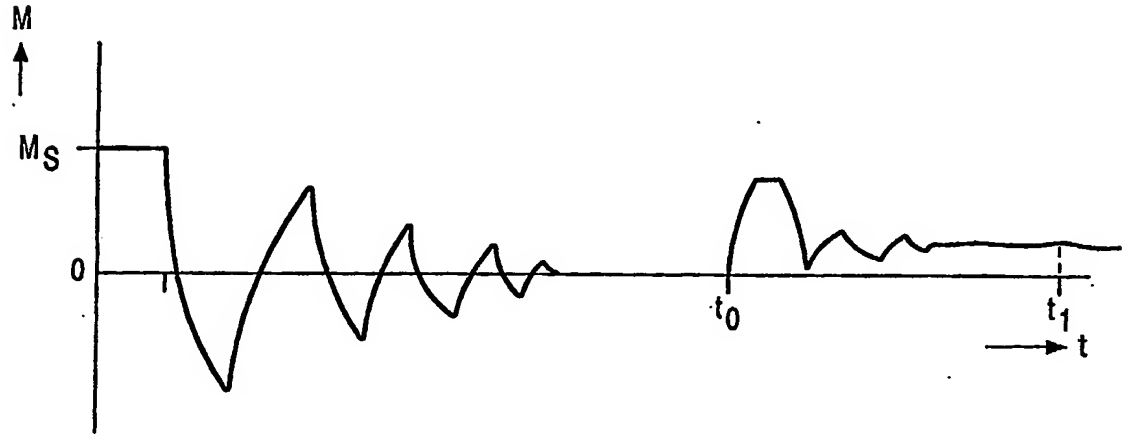

FIG. 6B

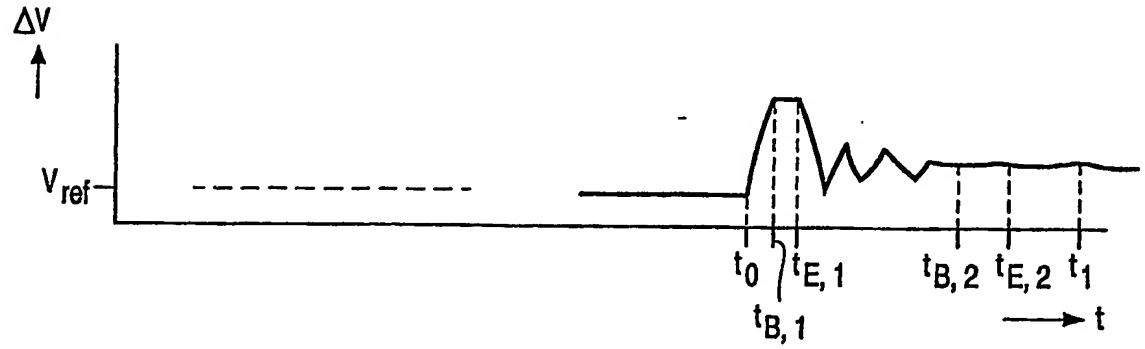

FIG. 6C

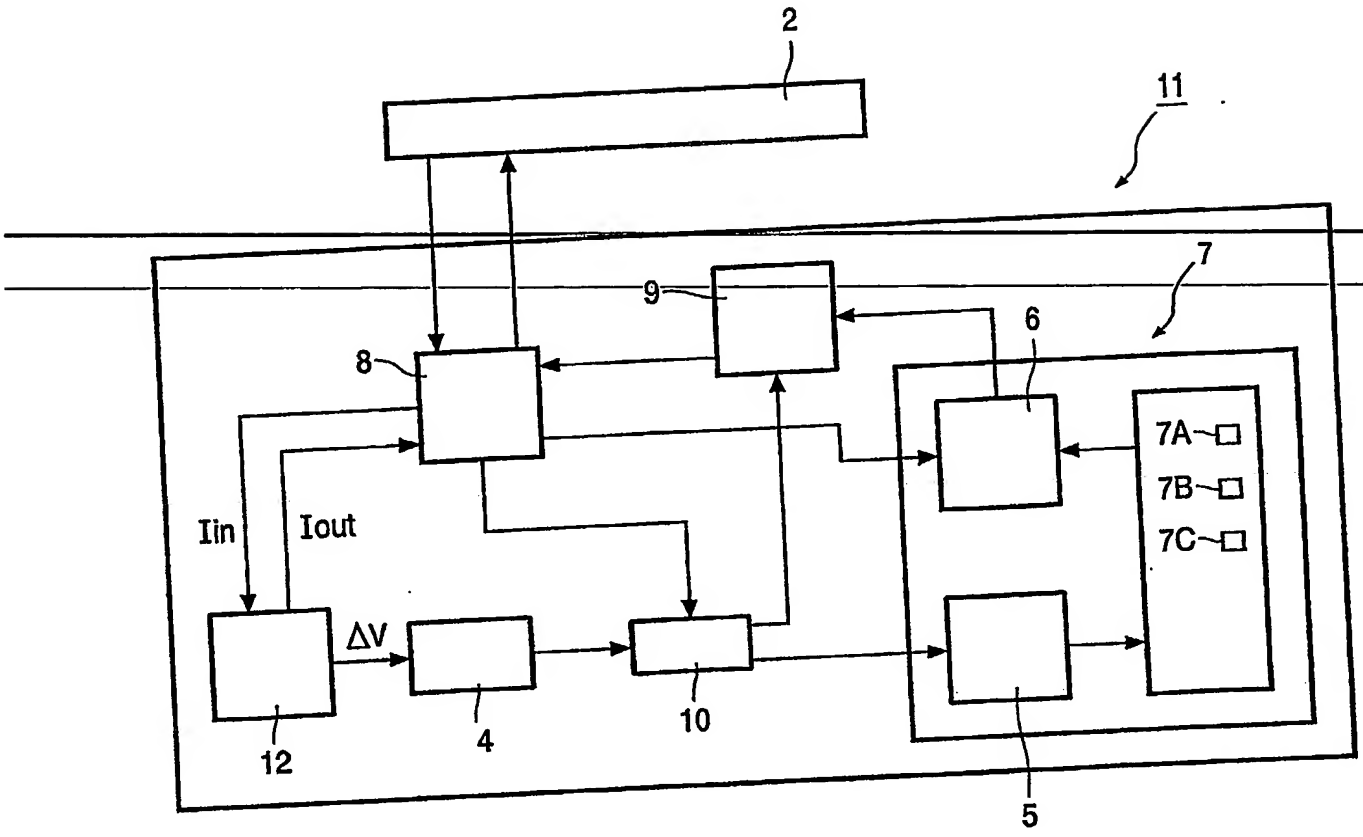

FIG. 7